інфраструктури. Використання хмарових технологій дозволяє збільшити ефективність обробки та зберігання великих обсягів інформації, забезпечуючи при цьому високий рівень безпеки та доступності.

Розвиток кіберфізичних систем, що поєднують в собі обчислювальні та фізичні компоненти, визначає новий етап технічної інфраструктури. Упровадження розумних міст, промислових об'єктів та транспортних систем збільшує автоматизацію та взаємодію між різними секторами, в той час забезпечуючи відповідні заходи кіберзахисту.

Під час розвитку технічної інфраструктури слід враховувати кібербезпеку як невід'ємну складову. Запровадження передових засобів шифрування, систем виявлення та протидії кіберзагрозам, а також регулярне оновлення кіберзахисних заходів, стає критичним для запобігання інцидентів та збереження стійкості систем [3, с. 23-28].

Отже, у змінливому світі кіберзагроз, Україна має активно реагувати на виклики, пов'язані із кібербезпекою, здійснюючи важливі кроки для захисту своїх інформаційних ресурсів та критичних інфраструктур. Здійснення комплексних заходів, від розробки стратегії до підвищення обізнаності та технічного розвитку, є важливими кроками для забезпечення ефективного кіберзахисту. Тільки через співпрацю всіх зацікавлених сторін, Україна зможе відповісти на виклики кіберпростору та зберегти свою кібербезпеку в умовах постійної зміни технологічного ландшафту.

1. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право.* 2019. № 9. С. 100-108.

2. Богуш В. М. Кібербезпека та захист критичної інформаційної інфраструктури. *Правова інформатика.* 2015. № 2. С. 119-121.

3. Веселова Л. Особливості державної політики України у сфері забезпечення кібербезпеки в умовах гібридної війни. *Науковий вісник Херсонського державного університету.* Серія: «Юридичні науки». 2019. № 2. С. 23-28.

4. Геращенко Ю. Державна політика у сфері кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського.* Серія: «Державне управління». 2019. № 1. С. 140-145.

5. Даник Ю. Г. Основи кібербезпеки та кібероборони: підручник. Видання друге, перероб. та доп. Одеса.: ОНАЗ ім. О.С. Попова, 2019. 320 с.

УДК 004.738.5:351.862.4:341.31
DOI: 10.31733/15-03-2024/2/374-375

Артур ПАНТЮШЕНКО
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції

Олена БОЙКО
старший викладач кафедри
тактико-спеціальної підготовки
Дніпропетровського державного
університету внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ УКРАЇНИ ПІД ЧАС ВОЄННОГО СТАНУ В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Звертаючи увагу на виклики сьогодення перед Україною, захист прав, свобод, суверенітету і територіальної цілісності посідає значне місце. Підсилюючим фактором для захисту є військові дії на території України, які дуже сильно шкодять соціальному середовищу України. Крім того, зовнішні фактори це лише одна частина небезпеки для держави, оскільки існують і внутрішні фактори, такі як кібератаки, кіберзлочини, шахрайства на гуманітарній основі, розкрадання державного майна шляхом проведення відкритих торгів з основою фіктивних публічних закупівель через сайт «Прозоро». Також, у зв'язку із військовою агресією, постає питання захисту персональних даних громадян у цифрову епоху, оскільки сьогодні дістати інформацію про особу через соціальні мережі чи інші сайти дуже проста задача для шахраїв та агентів. І тому нижче ми висвітлимо напрямки для підвищення ефективності інформаційного захисту.

Наразі зазначимо, що функції держави включають у себе функцію захисту. Відтак, згідно ст. 17 Конституції України: «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» [1].

Під інформаційною безпекою слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека має включати ефективну протидію сукупності інформаційних загроз [2]. Відтак, інформаційна безпека – являє собою нерозривну дуже важливу систему захисту держави у сфері обігу інформації, наприклад (політичної інформації або військової інформації), а також захист від потенційних зовнішніх та внутрішніх загроз, які себе можуть проявляти, як у просторі Інтернету, так і на передовій фронту України.

Отже, погоджуємось зі словами О. Довгань, а саме, що для успішного входження нашої держави в міжнародний інформаційний обмін вона має зосередитись насамперед у сфері правової діяльності за такими напрямками: розробити, розвинути та ввести в дію систему нормативно-правових актів, спрямованих на високий рівень захисту національних інформаційних ресурсів використання в національних інтересах; створити законодавчу базу для регулювання участі в міжнародній діяльності для забезпечення дотримання міжнародного інформаційного законодавства, такого як боротьба з кібертероризмом. [3].

Отже, враховуючи все вищесказане та спираючись на те, що дана тематика потребує більшої уваги з боку науковців та правотворчих органів можна дійти до висновку, що інформаційна безпека в Україні, є важливою складовою національної безпеки. І вище перелічені напрямки вдосконалення законодавства, є не вичерпними для збільшення інформаційного захисту у державі. І на сьогодні варто приділяти значну увагу цьому питанню та переходити у наступальні дії, особливо у зв'язку з кібератаками та дезінформацією ворога на передовій.

1. Конституція України URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text [дата звернення 26.02.2024]

2. Боднар, І. Р. Сучасні реалії інформаційного суспільства: проблеми становлення та перспективи розвитку: монографія. Львівської комерційної академії, 2013. 320 с.

3. Довгань О.Д. Організація правового гарантування безпеки інформаційних обмінів у контексті глобалізації. *Правова інформатика. № 4(40)*. 2013. С. 79-88.

УДК 355.451
DOI: 10.31733/15-03-2024/2/375-377

Ілля ПАРФЬОНОВ
курсант факультету підготовки
фахівців для підрозділів
кримінальної поліції

Валерій БІЛІЧЕНКО
старший викладач кафедри
тактико-спеціальної підготовки
Дніпропетровського державного
університету внутрішніх справ

РОЛЬ ТА ЕФЕКТИВНІСТЬ СИСТЕМ КОМУНІКАЦІЙ ТА КООРДИНАЦІЇ У СПЕЦІАЛЬНИХ ВІЙСЬКОВИХ ПІДРОЗДІЛАХ: АНАЛІЗ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ

У сучасній війні головне – швидкість та ефективність комунікації між підрозділами. Щоб ефективно вести війну, потрібно заохочувати інших громадян допомагати вести бойові дії – створювати речі, перевозити їжу, допомагати евакуювати цивільних людей з окупованих територій та інше.

Все це було б неможливо без сучасних методів комунікації. Потрібно швидко передавати інформацію, але так, щоб її не перехопив ворог. Для цього створили різні